UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/817,323	03/26/2001	Barry Lynn Royer	2001P04784Us	8853

7590 03/09/2006

Siemens Corporation
Intellectual Property Department
186 Wood Avenue South
Iselin, NJ 08830

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/817,323	ROYER ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20060119*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A reply under 37 CFR 1.116 was received on 25 May 2005. By this reply, no claims were amended, added, or canceled. A Notice of Appeal was received on 07 July 2005. An Appeal Brief was received on 08 September 2005 and a supplemental Appeal Brief was received on 14 December 2005. Claims 1-24 are currently pending in the present application.

Response to Arguments

2. In view of the supplemental Appeal Brief filed on 14 December 2005, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

E. Moise

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Information Disclosure Statement

3. The information disclosure statement received 19 January 2006 was received during the period set forth in 37 CFR 1.97(d) (i.e. after the mailing date of a final rejection). Applicant has paid the fee as required in 37 CFR 1.97(d)(2) but has not provided a statement under 37 CFR 1.97(e) as required by 37 CFR 1.97(d)(1). However, because prosecution is herein reopened, the Examiner has considered the above information disclosure statement as though it were filed under 37 CFR 1.97(c).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-9, 11-15, 18, 20, 21, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood, US Patent 5708780, in view of Calamera et al, US Patent 6463533.

In reference to Claim 1, Levergood discloses a system including an input processor that receives an encryption key (column 5, lines 61-65), a URL processor that adaptively processes a URL link to a second application by encrypting a URL portion (column 5, lines 61-65; column 3, lines 34-37; and column 4, lines 1-18) and by not further encrypting a link within the first application (column 3, lines 59-67), and a communication processor that includes the processed URL in web page data (column 6, lines 17-26). However, although Levergood discloses that the encrypted URL portion includes, *inter alia*, an accessible domain and an IP address of the user (see column 3, lines 34-37), Levergood does not explicitly disclose that the portion that is encrypted is the address portion of the URL.

Calamera discloses a system including a URL processor that encrypts an address portion of a URL (DOMAIN and PATH, column 8, lines 43-48) and a communication processor that includes the processed URL in web page data (ALIAS, column 8, lines 58-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood by including the encryption of the URL address portion, in order to allow tracking of the user across several application sites (see Calamera, column 2, lines 57-65).

In reference to Claim 2, Levergood and Calamera further disclose the encryption key is accessible to multiple applications from a managing application (Levergood,

column 5, lines 61-65, where the key is shared by the authentication and content servers; Calamera, Figure 3, Alias Server System 42, and column 5, lines 49-60).

In reference to Claim 3, Levergood and Calamera further disclose communicating the address portion to a managing application for encryption (Levergood, column 5, lines 44-49, for example, where the request is redirected to an authentication server; Calamera, Figure 3, Alias Server System 42, and column 8, lines 43-46).

In reference to Claim 4, Levergood and Calamera further disclose that the URL processor adaptively processes the URL link in response to an identified URL type (see Levergood, column 3, line 56-column 4, line 24).

In reference to Claim 5, Levergood and Calamera further disclose that a URL link can include an encrypted portion and a non-encrypted portion (Levergood, column 5, lines 52-54, where [SID] includes an encrypted digital signature; Calamera, column 8, lines 58-60).

In reference to Claim 6, Levergood and Calamera further disclose a browser application providing a user interface for providing user identification information (Levergood, column 6, lines 44-47; Calamera, ID, as defined in column 7, lines 35-36; also column 8, lines 8-10) and authenticating the user identification information (Levergood, column 6, lines 36-42; Calamera, column 8, lines 16-18).

In reference to Claims 7 and 8, Levergood and Calamera further disclose compressing the address portion with a hash function (Levergood, column 5, lines 61-65; Calamera, column 8, lines 48-50).

In reference to Claim 9, Levergood and Calamera further disclose communicating the address portion to a managing application for compression (Levergood, column 5, lines 44-49, for example, where the request is redirected to an authentication server; Calamera, Figure 3, Alias Server System 42, and column 8, lines 52-54).

In reference to Claim 11, Levergood discloses a system that includes a managing application providing a common encryption key to a plurality of applications (column 5, lines 61-65, where the key is shared by the authentication and content servers). Levergood further discloses an application including an input processor that receives an encryption key (column 5, lines 61-65), a URL processor that adaptively processes a URL link to a second application by encrypting a URL portion (column 5, lines 61-65; column 3, lines 34-37; and column 4, lines 1-18) and by not further encrypting a link within the first application (column 3, lines 59-67), and a communication processor that includes the processed URL in web page data (column 6, lines 17-26). However, although Levergood discloses that the encrypted URL portion includes, *inter alia*, an accessible domain and an IP address of the user (see column 3, lines 34-37), Levergood does not explicitly disclose that the portion that is encrypted is the address portion of the URL.

Calamera discloses a system including a managing application providing a common encryption key (Figure 3, Alias Server System 42, and column 5, lines 49-60) a URL processor that encrypts an address portion of a URL (DOMAIN and PATH, column

8, lines 43-48) and a communication processor that includes the processed URL in web page data (ALIAS, column 8, lines 58-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood by including the encryption of the URL address portion, in order to allow tracking of the user across several application sites (see Calamera, column 2, lines 57-65).

In reference to Claim 12, Levergood and Calamera further disclose communicating the address portion to the managing application for encryption (Levergood, column 5, lines 44-49, for example, where the request is redirected to an authentication server; Calamera, Figure 3, Alias Server System 42, and column 8, lines 43-46).

In reference to Claims 13 and 14, Levergood and Calamera further disclose compressing the address portion with a hash function (Levergood, column 5, lines 61-65; Calamera, column 8, lines 48-50).

In reference to Claim 15, Levergood and Calamera further disclose communicating the address portion to the managing application for compression (Levergood, column 5, lines 44-49, for example, where the request is redirected to an authentication server; Calamera, Figure 3, Alias Server System 42, and column 8, lines 52-54).

In reference to Claim 18, Levergood discloses an application including a URL processor that adaptively processes a URL link to a second application by encrypting a

URL portion (column 5, lines 61-65; column 3, lines 34-37; and column 4, lines 1-18) and by not further encrypting a link within the first application (column 3, lines 59-67), and a communication processor that includes the processed URL in web page data (column 6, lines 17-26). However, although Levergood discloses that the encrypted URL portion includes, *inter alia*, an accessible domain and an IP address of the user (see column 3, lines 34-37), Levergood does not explicitly disclose that the portion that is encrypted is the address portion of the URL.

Calamera discloses a system including a URL processor that encrypts an address portion of a URL (DOMAIN and PATH, column 8, lines 43-48) and a communication processor that includes the processed URL in web page data (ALIAS, column 8, lines 58-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood by including the encryption of the URL address portion, in order to allow tracking of the user across several application sites (see Calamera, column 2, lines 57-65).

In reference to Claim 20, Levergood discloses a system including a browser that includes a user interface for providing user identification information (column 6, lines 44-47), a URL generator for generating a URL with an encrypted URL portion (column 5, lines 61-65) and a session identifier (see, for example, column 3, lines 11-16), and a processor communicating the generated URL once the user identification information is validated (column 6, lines 44-57), where the application receiving the URL has access to the key (column 5, lines 61-65, where the key is shared by the authentication and

content servers). However, although Levergood discloses that the encrypted URL portion includes, *inter alia*, an accessible domain and an IP address of the user (see column 3, lines 34-37), Levergood does not explicitly disclose that the portion that is encrypted is the address portion of the URL.

Calamera discloses a system including a browser that includes a user interface for providing user identification information (column 6, lines 8-10), a URL generator that generates a URL with an encrypted address portion (DOMAIN and PATH, column 8, lines 43-48), and a processor communicating the generated URL once the user identification information is validated (column 8, lines 16-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood by including the encryption of the URL address portion, in order to allow tracking of the user across several application sites (see Calamera, column 2, lines 57-65).

Claims 21 and 23 are directed to methods corresponding substantially to the systems of Claims 1 and 11, respectively, and are rejected by a similar rationale.

In reference to Claim 24, Levergood discloses a method including adaptively processing a URL link to a second application by encrypting a URL portion (column 5, lines 61-65; column 3, lines 34-37; and column 4, lines 1-18) and by not further encrypting a link within the first application (column 3, lines 59-67), providing a key to the second application (column 5, lines 61-65, where the key is shared by the

authentication and content servers), and including the generated URL in web page data (column 6, lines 17-26). However, although Levergood discloses that the encrypted URL portion includes, *inter alia*, an accessible domain and an IP address of the user (see column 3, lines 34-37), Levergood does not explicitly disclose that the portion that is encrypted is the address portion of the URL.

Calamera discloses a method including encrypting an address portion of a URL (DOMAIN and PATH, column 8, lines 43-48) and including the processed URL in web page data (ALIAS, column 8, lines 58-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Levergood by including the encryption of the URL address portion, in order to allow tracking of the user across several application sites (see Calamera, column 2, lines 57-65).

6. Claims 10, 16, 17, 19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood in view of Calamera and further in view of Berman, US Patent 5995939.

In reference to Claim 10, Levergood and Calamera disclose everything as applied to Claim 1 above. Levergood and Calamera further disclose encrypting a user identifier (Levergood, column 3, lines 34-37, noting that the SID includes a user identifier that is included under the digital signature; Calamera, ID in column 8, lines 56-58). However, neither Levergood nor Calamera explicitly discloses encrypting patient information for inclusion in the URL. Berman discloses a system that includes

compressing and encrypting messages containing patient specific information (column 6, lines 2-15). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood and Calamera by including patient data as the user information that is encrypted and compressed, in order to ensure the confidentiality of sensitive data (see Berman, column 2, lines 61-63).

In reference to Claim 16, Levergood discloses a system including a browser application providing a user interface for providing user identification information (column 6, lines 44-47). Levergood further discloses an application including a URL processor that encrypts a URL portion (column 5, lines 61-65; column 3, lines 34-37; and column 4, lines 1-18) and a communication processor that includes the processed URL in web page data (column 6, lines 17-26). However, although Levergood discloses that the encrypted URL portion includes, *inter alia*, an accessible domain and an IP address of the user (see column 3, lines 34-37), Levergood does not explicitly disclose that the portion that is encrypted is the address portion of the URL.

Calamera discloses a system including a browser that includes a user interface for providing user identification information (column 6, lines 8-10), a URL processor that encrypts an address portion of a URL (DOMAIN and PATH, column 8, lines 43-48), and a communication processor that includes the processed URL in web page data (ALIAS, column 8, lines 58-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood by

including the encryption of the URL address portion, in order to allow tracking of the user across several application sites (see Calamera, column 2, lines 57-65).

Additionally, Levergood and Calamera further disclose encrypting a user identifier (Levergood, column 3, lines 34-37, noting that the SID includes a user identifier that is included under the digital signature Calamera, ID in column 8, lines 56-58); however, neither Levergood nor Calamera explicitly discloses encrypting patient information for inclusion in the URL. Berman discloses a system that includes compressing and encrypting messages containing patient specific information (column 6, lines 2-15). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood and Calamera by including patient data as the user information that is encrypted and compressed, in order to ensure the confidentiality of sensitive data (see Berman, column 2, lines 61-63).

In reference to Claim 17, Levergood and Calamera further disclose communicating information to another application for encryption (Levergood, column 5, lines 44-49, for example, where the request is redirected to an authentication server; Calamera, Figure 3, Alias Server System 42, and column 8, lines 43-46).

In reference to Claim 19, Levergood and Calamera disclose everything as applied to Claim 18 above. Levergood and Calamera further disclose encrypting a user identifier (Levergood, column 3, lines 34-37, noting that the SID includes a user identifier that is included under the digital signature Calamera, ID in column 8, lines 56-58). However, neither Levergood nor Berman explicitly discloses encrypting patient

information for inclusion in the URL. Berman discloses a system that includes compressing and encrypting messages containing patient specific information (column 6, lines 2-15). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Levergood and Calamera by including patient data as the user information that is encrypted and compressed, in order to ensure the confidentiality of sensitive data (see Berman, column 2, lines 61-63).

In reference to Claim 22, Levergood discloses a method including enabling a first application based on validation of user authentication information (column 6, lines 36-42), forming a URL by encrypting a link to a second application and including the encrypted link and session identification information in the formed URL (column 5, lines 52-54 and 61-65), including the link in data representing a web page, and communicating the web page data (column 6, lines 17-26). However, although Levergood discloses that the encrypted URL link includes, *inter alia*, an accessible domain and an IP address of the user (see column 3, lines 34-37), Levergood does not explicitly disclose that the portion that is encrypted is the link address.

Calamera discloses a method including enabling an application based on validation of user authentication information (column 8, lines 16-18), forming a URL by encrypting a link address of a URL (DOMAIN and PATH, column 8, lines 43-48), and including the formed URL in web page data and communicating the web page data (column 8, lines 58-60). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Levergood by

including the encryption of the URL address portion, in order to allow tracking of the user across several application sites (see Calamera, column 2, lines 57-65).

Additionally, Levergood and Calamera further disclose encrypting a user identifier (Levergood, column 3, lines 34-37, noting that the SID includes a user identifier that is included under the digital signature Calamera, ID in column 8, lines 56-58); however, neither Levergood nor Calamera explicitly discloses encrypting patient information for inclusion in the URL. Berman discloses a method that includes compressing and encrypting messages containing patient specific information (column 6, lines 2-15). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Levergood and Calamera by including patient data as the user information that is encrypted and compressed, in order to ensure the confidentiality of sensitive data (see Berman, column 2, lines 61-63).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Payne et al, US Patent 5715314, discloses a system in which URLs and various data fields in the URL are encrypted and signed to form an authenticator that is used to validate the URLs.

b. Binding et al, US Patent 6751731, discloses a system in which encrypted parameters for establishing security may be appended to a URL request (see especially column 12).

c. Ganesan et al, US Patent 6948063, discloses a system that protects the integrity of URLs using encryption and/or hashing.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER